UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,459	12/29/2003	Bing Wang	059643.00747	7057

32294 7590 12/08/2008

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
MAI, KEVIN S	

ART UNIT	PAPER NUMBER
2456	

MAIL DATE	DELIVERY MODE
12/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/748,459	WANG, BING	
	Examiner	Art Unit	
	KEVIN S. MAI	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action has been issued in response to Applicant's Amendment filed August 29, 2008.

2. Claims 24 and 25 have been added. Claim 3 has been canceled. Claims 1, 4, 5, 8-15, 18, 19 and 21-23 have been amended. Claims 1, 2 and 4-25 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed August 29, 2008 have been fully considered but they are not persuasive.

4. Applicant's arguments with respect to claim 1 have been fully considered but they are not persuasive. Applicant argues the unified session manager is different from the SEP in Araujo because the unified session manager is capable of modifying a request and does not need to be part of the network device. In addition, the unified session manager can also perform authentication of the user and directly manage the network device or allow it to be managed by a separate management server. Further, applicant states Araujo certainly does not disclose or suggest establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device. Applicant argues that examiners alleged attempt to justify that the connection is transparent to the user is without merit, and that there is no correlation between the SEP and the unified session manager because the SEP is part

of the virtual office server and the unified session manager is separate from a management server. Then applicant insists that the configuration offered by Araujo is clearly different because the unified session manager and the management server are separate devices. Then the single device could not possibly produce the outcome of the claimed subject matter which provides transparent authentication between a unified session manager and a management server. These are the arguments made by applicant as to why Araujo does not disclose applicant's invention.

Examiner disagrees and also asserts that some of the arguments are toward information that is not actually claimed and are only limitations in the specification. For example the need for the unified session manager to be separate from the management servers is not distinctly claimed. Examiner disagrees for the following reasons –

- Applicant argues the unified session manager is different from the SEP because the unified session manager is capable of modifying a request and does not need to be part of the network device. Araujo does disclose modifying a request, paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user. Namely converting the messages is seen to be modifying requests. Then as to the SEP being part of the network device, applicant suggests that since SEP is in the **Virtual** Office Server, that it is part of the network device. However, since the office server is **virtual** it is seen that the office server is simply a representation and

the actual network devices that hold the applications are the servers in the 70 box as seen in figure 1. Furthermore, paragraph [0082] discloses the SEP and the servers being contained on separate computers, thus the SEP and servers are distinct from each other and not a singular device known as Virtual office server.

- Applicant argues the unified session manager can perform authentication of the user and directly manage the network device or allow it to be managed by a separate management server. Araujo does disclose the SEP performing authentication of the user, paragraph [0121] of Araujo discloses the SEP maintains lists of authorized user names and passwords, and, based on login information supplied by a user then seeking remote access, determining whether that user is permitted to access the applications. Thus based on the login information provided by the user, the SEP determines what the user is permitted to access. Araujo also discloses directly managing the network device or allowing it to be managed by a separate management server, however examiner does not feel this is claimed in the claim language. Araujo discloses this in paragraph [0101]; the SEP can contain a mail module if the SEP is used without an external e-mail server. Thus for e-mail it is seen that it could be directly managed by the SEP or managed by an external e-mail server.
- Applicant argues Araujo certainly does not disclose or suggest establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device. Araujo

discloses establishing a session, paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session). Then as to the establishing a session needing authentication, it is seen that Araujo does not explicitly disclose it however it is indeed suggested and in fact obvious in view of Araujo's disclosure. Paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other.

- Applicant argues that examiners alleged attempt to justify that the connection is transparent to the user is without merit, and that there is no correlation between the SEP and the unified session manager because the SEP is part of the virtual office server and the unified session manager is separate from a management server. Examiner asserts that the establishment of a connection between the SEP and the applications servers being transparent to the user is correct. Since the remote client is not part of the connection between the SEP and the applications servers, there is no

participation of the client in the establishment process. Thus is it seen that the establishment is transparent to the user. Then as to the unified session manager being distinct from the SEP because the SEP is part of a **virtual** office server, paragraph [0082] discloses the SEP and the servers being contained on separate computers, thus the SEP and servers are distinct from each other and not a singular device known as Virtual office server.

- Applicant argues that the configuration offered by Araujo is clearly different because the unified session manager and the management server are separate devices and the single device could not possibly produce the outcome of the claimed subject matter which provides transparent authentication between a unified session manager and a management server. Paragraph [0082] discloses the SEP and the servers being contained on separate computers, thus the SEP and servers are distinct from each other and not a singular device known as Virtual office server. Thus the SEP and the servers are separate devices. As such since they are separate devices it is seen that they can produce the outcome of the claimed subject matter.

Claim Objections

5. Claims 10 and 17 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claims 10 and 17 appear to no longer further limit claims 8 and 15 in view of the amendments made to claims 8 and 15.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claim 25 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 25 recites computer readable medium, however according to applicant's specification it appears that this can include signals. As such claim 25 appears to be claiming non-statutory subject matter.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 2 and 4-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo").

10. **As to Claim 1,** Araujo discloses **a method, comprising:**

receiving a request from a client device for access to an application associated with a network device (Paragraph [0084] of Araujo discloses the user can then click on any of these

icons (request), which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application);

establishing a session between a unified session manager and a management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device;**

modifying the request at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

forwarding, by the unified session manager, the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

receiving a response at the unified session manager from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120]

discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

modifying the response at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user); **and**

forwarding, by the unified session manager, the modified response to the client device (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

Araujo does not explicitly disclose, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP

and application servers would authenticate each other, wherein the authentication is transparent to the client.

11. **As to Claim 2,** Araujo discloses the invention as claimed as described in claim 1, **wherein the request is authenticated by the unified session manager** (Paragraph [0121] of Araujo discloses the SEP maintains lists of authorized user names and passwords, and, based on login information supplied by a user then seeking remote access, determining whether that user is permitted to access the applications)**.**

12. **As to Claim 4,** Araujo discloses the invention as claimed as described in claim 1, **wherein modifying the request further comprises translating a graphical user interface message and, wherein modifying the response further comprises translating another graphical user interface message** (Paragraph [0120] of Araujo discloses receiving user mouse clicks and keystrokes from the user browser in AIP form and translating them to RDP. Where clicks are seen include clicking on icons to cause applications to open and thus seen to be GUI messages (paragraph [0084]). Then paragraph [0120] discloses receiving graphical output displays from the client application in RDP and translating them to AIP)**.**

13. **As to Claim 5,** Araujo discloses the invention as claimed as described in claim 4, **wherein at least one of the graphical user interface message and the other graphical user interface message is translated into a unified format (**Paragraph [0120] of Araujo discloses the requests being converted from AIP form to RDP and then the responses being converted

from RDP form to AIP. These are both seen to be the GUI messages being translated into unified formats).

14. **As to Claim 6,** Araujo discloses the invention as claimed as described in claim 1, **wherein modifying the request further comprises modifying a network address before forwarding the modified request, and wherein modifying the response further comprises modifying another network address before forwarding the modified response** (Paragraph [0092] of Araujo discloses the SEP can intercept incoming network messages and perform required protocol conversion and IP address translation on each message and provide the opposite functionality in a reverse direction for outgoing messages. This is further clarified in paragraph [0097]).

15. **As to Claim 7,** Araujo discloses the invention as claimed as described in claim 1, **wherein modifying the response further comprises enabling a download of a file from the unified session manager** (Paragraph [0084] of Araujo discloses after a user clicks an icon to launch an application the SEP will launch the associated office application and generate an HTML file for graphical display produced by that application and then download the HTML file to the users browser).

16. **As to Claim 8,** Araujo discloses **an apparatus, comprising:**
a transceiver configured to receive a request from a client for access to an application on the network device and to forward a response to the request (Figure 2 of Araujo discloses a

set of Ethernet ports on the SEP. Paragraph [0120] discloses the SEP taking in requests from the client and sending responses back to the client)**; and**

a processor (Figure 2 and paragraph [0091] of Araujo disclose the SEP having a microprocessor)**, coupled to the transceiver, that is configured to**

establish a session on behalf of the client between the unified session manager and a management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)))). Araujo does not explicitly disclose**, wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device,**

modify the request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**,**

forward the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**,**

receive the response on behalf of the client from the management server associated with the application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user),

modify the response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user), **and**

forward the modified response from the management server to the transceiver (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

Araujo does not explicitly disclose wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the

SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

17. **As to Claim 9,** Araujo discloses the invention as claimed as described in claim 8, **wherein the processor is further configured to authenticate the request** (Paragraph [0121] of Araujo discloses the SEP maintains lists of authorized user names and passwords, and, based on login information supplied by a user then seeking remote access, determining whether that user is permitted to access the applications).

18. **As to Claim 10,** Araujo discloses the invention as claimed as described in claim 8, **wherein the processor is further configured to authenticate to the management server, and wherein the authentication is virtually transparent to the client** (Paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it).

19. **As to Claim 11,** Araujo discloses the invention as claimed as described in claim 10, **wherein the authentication to the management server further comprises sending at least one of a password, a certificate, and an encryption key** (Paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. SSL is known to utilize certificates and encryption keys in its authentication process and thus it is seen that the authentication between the SEP and the Application server comprises those things).

20. **As to Claim 12,** Araujo discloses the invention as claimed as described in claim 8, **wherein the processor is further configured to modify at least one of the request and the response by translating at least one graphical user interface message** (Paragraph [0120] of Araujo discloses receiving user mouse clicks and keystrokes from the user browser in AIP form and translating them to RDP. Where clicks are seen include clicking on icons to cause applications to open and thus seen to be GUI messages (paragraph [0084]). Then paragraph [0120] discloses receiving graphical output displays from the client application in RDP and translating them to AIP).

21. **As to Claim 13,** Araujo discloses the invention as claimed as described in claim 8, **the processor is further configured to**
establish another session on behalf of the client with another application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session). As to it being another session Paragraph [0084] discloses

the user can readily move between one remote office application to the next by simply clicking on the associated icon, this further applies to the remaining limitations);

modify another request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

forward the other modified request to the application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

receive another response on behalf of the client from the application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

modify the other response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user); **and**

forward the other modified response to the transceiver (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator

to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

22. **As to Claim 14,** Araujo discloses the invention as claimed as described in claim 8, **wherein the processor is further configured to enable a plurality of clients to access virtually simultaneously a plurality of applications on the network device** (Paragraph [0077] of Araujo discloses the SEP can simultaneously accommodate multiple clients. Then paragraph [0084] discloses the SEP allowing the user to readily move between one remote office application to another).

23. **As to Claim 15,** Araujo discloses **a method comprising: establishing a session between a unified session manager and at least one of a plurality of the management servers, wherein the unified session manager is enabled to operate on behalf of at least one of a plurality of clients** (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session). As to there being a plurality of management servers, paragraph [0084] discloses the user can readily move between office applications by clicking on associated icons, thus there are a plurality of management servers. Then as to there being a plurality of clients, paragraph [0077] of Araujo discloses the SEP can simultaneously accommodate multiple clients). Araujo does not explicitly disclose**, and wherein establishing the session with the at**

least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients; and

modifying each message from the at least one of the plurality of clients destined for an application associated with the at least one of the plurality of the management servers, wherein the modification is virtually transparent to the client and to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application).

Araujo does not explicitly disclose, and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

24. **As to Claim 16,** Araujo discloses the invention as claimed as described in claim 15, **wherein the unified session manager is enabled to operate on behalf of each of the plurality of clients seeking access to the at least one of the plurality of management servers** (Paragraph [0077] of Araujo discloses the SEP can simultaneously accommodate multiple clients. Then paragraph [0084] discloses the SEP allowing the user to readily move between one remote office application to another)**.**

25. **As to Claim 17,** Araujo discloses the invention as claimed as described in claim 15, **wherein establishing the session between the unified session manager and the at least one of the plurality of the management servers further comprises performing an authentication to the at least one of the plurality of the management servers, and wherein the authentication is virtually transparent to the at least one of the plurality of the clients** (Paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it)**.**

26. **As to Claim 18,** Araujo discloses the invention as claimed as described in claim 15, **wherein modifying each message between the at least one of the plurality of the clients and the at least one of the plurality of the management servers further comprises at least one of**

wrapping a Java applet (Figure 11 of Araujo discloses using a Java Applet (1180)), **and translating a uniform resource locator** (Paragraph [0036] of Araujo discloses the SEP taking in input in the form of URI/URL selection).

27. **As to Claim 19,** Araujo discloses **a method, comprising:**

retrieving a set of menu entries including at least one menu entry that is associated with a remote application (Figure 18 of Araujo discloses displaying to the user the applications available to them);

displaying a selection menu on a display comprising the set of menu entries (Figure 18 of Araujo discloses displaying to the user the applications available to them);

retrieving a menu entry selection signal, wherein the menu entry selection signal is modified by a unified session manager (Paragraph [0084] of Araujo discloses the user can click on any of the application icons to cause the SEP to launch the associated office application. Then paragraph [0120] discloses how mouse clicks are sent in AIP form and converted to RDP by the SEP);

forwarding the modified menu entry selection signal to a management server associated with the remote application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

receiving another signal indicative of a response from the management server, wherein the other signal is modified by the unified session manager (Paragraph [0086] of Araujo discloses

the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

establishing a session between the unified session manager and the management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device; and**

displaying the other modified signal at the display (Paragraph [0120] of Araujo discloses the screen shots from the application are sent to the user to be rendered by the user's browser)**.**

Araujo does not explicitly disclose wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo

discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

28. **As to Claim 20,** Araujo discloses the invention as claimed as described in claim 19, **wherein the menu entry selection signal comprises, a request for authentication, and a request for a program download** (Paragraph [0084] of Araujo discloses how a user must first login to be authorized to do anything, wherein the act of logging in is seen as having been authenticated. Then paragraph [0154] discloses when a user clicks on the "My Apps" tab an HTML page that contains a Java applet is downloaded to the browser, wherein the java applet is seen to be the program).

29. **As to Claim 21,** Araujo discloses the invention as claimed as described in claim 19, **wherein modifying the menu entry selection signal further comprises translating a graphical user interface message** (Paragraph [0120] of Araujo discloses receiving user mouse clicks and keystrokes from the user browser in AIP form and translating them to RDP. Where clicks are seen include clicking on icons to cause applications to open and thus seen to be GUI messages (paragraph [0084])), **altering a network address** (Paragraph [0092] of Araujo discloses the SEP can intercept incoming network messages and perform required protocol conversion and IP address translation on each message and provide the opposite functionality in a reverse direction for outgoing messages. This is further clarified in paragraph [0097]), **and attaching additional information to the signal** (Paragraph [0110] of Araujo discloses

performing SSL operations on the data. This is seen to be adding additional information to the signal).

30. **As to Claim 22,** Araujo discloses the invention as claimed as described in claim 19, **wherein modifying the other signal, indicative of a response from the management server, further comprises translating a graphical user interface message** (Paragraph [0120] or Araujo discloses receiving graphical output displays from the client application in RDP and translating them to AIP), **altering a network address** (Paragraph [0092] of Araujo discloses the SEP can intercept incoming network messages and perform required protocol conversion and IP address translation on each message and provide the opposite functionality in a reverse direction for outgoing messages. This is further clarified in paragraph [0097]), **and attaching additional information to the signal** (Paragraph [0111] of Araujo discloses using the Open SSL module to provide appropriate security functions to the response. This is seen to be adding additional information to the signal).

31. **As to Claim 23,** Araujo discloses **an apparatus, comprising:**
a means for establishing a session with a management server associated with an application on behalf of a remote client (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the**

management server, wherein the authenticating means is virtually transparent to the client;

a means for modifying the request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

a first forwarding component configured to forward the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

a means for receiving a response from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

a means for modifying the response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user); **and**

a second forwarding component configured to forward the modified response to the remote client (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

Araujo does not explicitly disclose, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

32. **As to Claim 24,** Araujo discloses **an apparatus, comprising:**

an establisher configured to establish a session with a management server associated with an application on behalf of a remote client (Paragraph [0084] of Araujo discloses the user can

then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose, **wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client;**

a modifier configured to modify a request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

a request forwarder configured to forward the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

a receiver configured to receive a response from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

a modifier configured to modify the response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical

output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**; and**

a response forwarder configured to forward the modified response to the remote client (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**.**

Araujo does not explicitly disclose wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

33. **As to Claim 25,** Araujo discloses **a computer program embodied on a computer readable medium, said computer program configured to control a processor to perform:**

receiving a request from a client device for access to an application associated with a network device (Paragraph [0084] of Araujo discloses the user can then click on any of these icons (request), which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application);

establishing a session between a unified session manager and a management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose, **wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device;**

modifying the request at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

forwarding, by the unified session manager, the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

receiving a response at the unified session manager from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications

and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

modifying the response at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user); **and**

forwarding, by the unified session manager, the modified response to the client device (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

Araujo does not explicitly disclose, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo

discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

Conclusion

34. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

35. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 20080086564 A1 - Communication application server for converged communication services to Putman; Janis Rae et al.

US 6938076 B2 - System, computer product and method for interfacing with a private communication portal from a wireless device to Meyer; Steven P et al.

US 20080028061 A1 - Managed Services Platform to Hartman; Robert Charles et al.

US 20050216847 A1 - Distributed document sharing to Zhu, Min et al.

US 20050010667 A1 - System and method for resource accounting on computer network to Moriki, Toshiomi et al.

US 20040267905 A1 - Managing network-accessible accounts to McDonough, John et al.

US 20040122925 A1 - Enabling access to an application through a network portal to Offermann, Udo

US 7020697 B1 - Architectures for netcentric computing systems to Goodman; Marina et al.

US 6950990 B2 - Navigation tool for accessing workspaces and modules in a graphical user interface to Rajarajan; Vij et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The examiner can normally be reached on Monday through Friday 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KSM

/Philip C Lee/
Primary Examiner, Art Unit 2452